IN THE CLAIMS:

Please amend claims 13-21 and 29-36, and add claim 37 as follows.

1. (Previously Presented) A method, comprising:

receiving a message from a terminal device connected to a packet data network;

deriving a first source information from said message;

deriving a second source information;

comparing said first source information and second source information;

initiating a protection processing based on a result of said comparing; and

providing secure access to said packet data network based on said protection processing.

2. (Cancelled)

3. (Previously Presented) The method according to claim 1, wherein said second source information is a source address information derived from a packet data unit configured to convey said message, or from a security association set up between said terminal device and said packet data network.

4. (Previously Presented) The method according to claim 1, wherein said protection processing comprises a processing for dropping said message if the result of said comparing is that said first source information and said second source information do not indicate the same location.

5. (Previously Presented) The method according to claim 1, wherein said protection processing comprises a processing for dropping said message if said comparing leads to the result that said first source information and said second source information do not match.

6. (Previously Presented) The method according to claim 1, wherein said first source information is an internet protocol address.

7. (Previously Presented) The method according to claim 6, wherein said message is a session initiation protocol message.

8. (Previously Presented) The method according to claim 1, wherein said second source information is at least a part of an internet protocol source address of an internet protocol datagram.

9. (Cancelled)

10. (Previously Presented) The method according to claim 3, wherein said second source information is an internet protocol address bound to an integrity key of said security association.

11. (Previously Presented) The method according to claim 10, wherein said internet protocol address is stored in a database of a proxy server configured to route said message to said packet data network.

12. (Previously Presented) The method according to claim 10, wherein said message is conveyed using a session initiation protocol level protection function.

13. (Currently Amended) ~~A network element~~An apparatus, comprising:

a receiving unit configured to receive a message from a terminal device connected to said network element;

a deriving unit configured to derive a first source information from said message, and to derive a second source information;

a comparing unit configured to compare said first source information and second source information; and

a protecting unit configured to initiate a protection processing based on a comparing result of said comparing unit and to provide secure access to a packet data network based on said protection processing.

14. (Currently Amended) The ~~network element~~apparatus according to claim 13, wherein said deriving unit is configured to derive said second source information from a packet data unit configured to derive said message or from a security association set up between said terminal device and said ~~network element~~apparatus.

15. (Currently Amended) The ~~network element~~apparatus according to claim 13, wherein said deriving unit is configured to derive said first source information from a header portion of said message.

16. (Currently Amended) The ~~network element~~apparatus according to claim 13, wherein said protecting unit is configured to initiate a processing for dropping said message if said comparing result indicates that said first source information and said second source information do not indicate a same location.

17. (Currently Amended) The ~~network element~~apparatus according to claim 13, wherein said protecting unit is configured to initiate a processing for dropping said message if said comparing result indicates that said first source information and said second source information do not match.

18. (Currently Amended) The ~~network element~~apparatus according to claim 13, wherein said deriving unit is configured to read said second source information from a database provided at said ~~network element~~apparatus.

19. (Currently Amended) The ~~network element~~apparatus according to claim 13, wherein said deriving unit is configured to derive said second source information by extracting an internet protocol source address from an internet protocol datagram.

20. (Currently Amended) The ~~network element~~apparatus according to claim 13, wherein said ~~network element~~apparatus is a proxy server.

21. (Currently Amended) The ~~network element~~apparatus according to claim 20, wherein said proxy server is a proxy call state control function of an internet protocol mobility subsystem.

22-28. (Cancelled)

29. (Currently Amended) The ~~network element~~apparatus according to claim 14, wherein said deriving unit is configured to derive said first source information from a header portion of said message.

30. (Currently Amended) The ~~network element~~apparatus according to claim 14, wherein said protecting unit is configured to initiate a processing for dropping said message if said comparing result indicates that said first source information and said second source information do not indicate the same location.

31. (Currently Amended) The ~~network element~~apparatus according to claim 14, wherein said protecting unit is configured to initiate a processing for dropping said message

if said comparing result indicates that said first source information and said second source information do not match.

32. (Currently Amended) The ~~network element~~apparatus according to claim 14, wherein said deriving unit is configured to read said second source information from a database provided at said ~~network element~~apparatus.

33. (Currently Amended) The ~~network element~~apparatus according to claim 14, wherein said deriving unit is configured to derive said second source information by extracting an internet protocol source address from an internet protocol datagram.

34. (Currently Amended) The ~~network element~~apparatus according to claim 14, wherein said ~~network element~~apparatus is a proxy server.

35. (Currently Amended) The ~~network element~~apparatus according to claim 34, wherein said proxy server is a proxy call state control function of an internet protocol mobility subsystem.

36. (Currently Amended) ~~A network element~~An apparatus, comprising:

receiving means for receiving a message from a terminal device connected to said network element;

deriving means for deriving a first source information from said message, and for deriving a second source information;

comparing means for comparing said first source information and second source information; and

protecting means for initiating a protection processing based on a comparing result of said comparing means and for providing secure access to a packet data network based on said protection processing.

37. (New) A computer program embodied on a computer-readable medium, the computer program configured to control a processor to perform operations comprising:

receiving a message from a terminal device connected to a packet data network;

deriving a first source information from said message;

deriving a second source information;

comparing said first source information and second source information;

initiating a protection processing based on a result of said comparing; and

providing secure access to said packet data network based on said protection processing.